Demo Internal Pentest

ACTIVITY REPORT

Cyology Demo

May 29, 2024

Copyright

© Cyology Labs. All Rights Reserved. This is unpublished material and contains trade secrets and other confidential information and is subject to a confidentiality agreement. The unauthorized possession, use, reproduction, distribution, display, or disclosure of this material or the information contained herein is prohibited.

The methodology used to audit the computer systems is considered proprietary intellectual information of Cyology Labs and may not be disclosed without written permission from CUSTOMERNAME. Cyology Labs gives permission to copy this report for the purpose of disseminating information within your organization, or any regulatory agency.

Assessment Project Team

Below is a list of contacts that were involved in this engagement. Should you have any questions pertaining to the content of this document or any project and non-project-related items, please feel free to reach out to the necessary project contacts.

Primary Point of Contact	
Name:	Terry Cutler
Title:	CEO & Ethical Hacker
Office:	(844) CYOLOGY (296-5649)
Email:	support@cyologylabs.com

Activity Log

This section of the report will contain detailed and specific information about the activities that were performed as part of the assessment. Using the information in this section, Cyology Labs recommends that CUSTOMERNAME evaluate technical security controls (e.g. detection and monitoring tools) to determine if any alerts have been triggered or activities have been logged.

Internal Network Penetration Test

Activity Time	Activity Type	Activity
10/09/2024 09:17AM CT	host discovery	Discovery module initiated.
10/09/2024 09:17AM CT	host discovery	Port scan module initialized.
10/09/2024 09:17AM CT	host discovery	MITRE | ATT&CK Conducting port scan against in-scope systems.
10/09/2024 09:17AM CT	host discovery	Running nmap port scans.
10/09/2024 09:17AM CT	host discovery	Completed nmap port scans.
10/09/2024 09:17AM CT	host discovery	Port scans completed successfully.
10/09/2024 09:17AM CT	host discovery	Parsing results for alive systems.
10/09/2024 09:17AM CT	host discovery	Completed parsing Nmap results. 276 new IP addresses discovered and imported into DB.
10/09/2024 09:17AM CT	host discovery	Parsing nmap port scans.
10/09/2024 09:17AM CT	host discovery	Completed parsing port scans. Imported 1017 new ports.
10/09/2024 09:17AM CT	host discovery	Identifying hostnames for all discovered systems.
10/09/2024 09:17AM CT	host discovery	MITRE | ATT&CK Enumerating systems via ARP traffic.
10/09/2024 09:17AM CT	host discovery	Checking for egress filtering deficiencies.
10/09/2024 09:17AM CT	host discovery	Completed checking for egress filtering deficiencies.
10/09/2024 09:17AM CT	host discovery	Discovery module completed.
10/09/2024 09:17AM CT	enumeration	Enumeration module initialized.
10/09/2024 09:17AM CT	enumeration	Enumerating SSH services.
10/09/2024 09:17AM CT	enumeration	Reviewing SMTP services.
10/09/2024 09:17AM CT	enumeration	Scanning Telnet services.
10/09/2024 09:17AM CT	enumeration	Reviewing LDAP services.
10/09/2024 09:17AM CT	enumeration	Enumerating NFS shares.
10/09/2024 09:17AM CT	enumeration	Enumerating MSSQL services.
10/09/2024 09:17AM CT	enumeration	Enumerating RDP services.
10/09/2024 09:17AM CT	enumeration	Enumerating MySQL services.
10/09/2024 09:17AM CT	enumeration	Enumerating PostgreSQL services.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: ftp-anon.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: sshv1.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: smtp-open-relay.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: telnet-encryption.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: smb-vuln-ms17-010.

10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: ssh2-enum-algos.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: smb-enum-shares.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: ssh-auth-methods.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: nfs-showmount.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: ldap-rootdse.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: nfs-ls.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/mssql/mssql_ping.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: nfs-statfs.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/mysql/mysql_version.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/rdp/ms12_020_check.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/rdp/cve_2019_0708_bluekeep.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/postgres/postgres_version.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Running nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: ftp-anon.

10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: sshv1.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/mssql/mssql_ping.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/mysql/mysql_version.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/rdp/ms12_020_check.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: nfs-showmount.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: ldap-rootdse.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: smb-vuln-ms17-010.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: smtp-open-relay.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: telnet-encryption.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: nfs-ls.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: ssh2-enum-algos.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: nfs-statfs.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-put.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Completed enumerating MSSQL services.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Completed reviewing NFS shares.
10/09/2024 09:17AM CT	enumeration	Completed reviewing SMTP services.
10/09/2024 09:17AM CT	enumeration	Completed enumerating MySQL services.
10/09/2024 09:17AM CT	enumeration	Completed reviewing LDAP services.
10/09/2024 09:17AM CT	enumeration	Anonymous FTP identified on ten (10) systems.
10/09/2024 09:17AM CT	enumeration	Analyzing web services running on port 8090/tcp.
10/09/2024 09:17AM CT	enumeration	Analyzing web services running on port 81/tcp.

10/09/2024 09:17AM CT	enumeration	Analyzing web services running on port 8443/tcp.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/telnet/telnet_version.
10/09/2024 09:17AM CT	enumeration	Analyzing web services running on port 443/tcp.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: ssh-auth-methods.
10/09/2024 09:17AM CT	enumeration	Completed reviewing SSH services.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Completed enumerating VNC services on port 5900
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/rdp/cve_2019_0708_bluekeep.
10/09/2024 09:17AM CT	enumeration	The RDP enumeration module identified one (1) system potentially vulnerable to BlueKeep.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/postgres/postgres_version.
10/09/2024 09:17AM CT	enumeration	Completed enumerating RDP services.
10/09/2024 09:17AM CT	enumeration	Completed enumerating PostgreSQL services.
10/09/2024 09:17AM CT	enumeration	Analyzing web services running on port 8080/tcp.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Completed analyzing web services running on port 81/tcp.
10/09/2024 09:17AM CT	enumeration	Completed reviewing HTTP services.
10/09/2024 09:17AM CT	enumeration	Completed enumerating FTP services on 10 IPs.
10/09/2024 09:17AM CT	enumeration	Completed analysis of FTP files.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/ftp/ftp_version.
10/09/2024 09:17AM CT	enumeration	Completed analyzing web services running on port 8443/tcp.
10/09/2024 09:17AM CT	enumeration	Completed analyzing web services running on port 8090/tcp.
10/09/2024 09:17AM CT	enumeration	Completed checking OWA web apps for the ProxyShell vulnerability.
10/09/2024 09:17AM CT	enumeration	Completed reviewing HTTPS services.
10/09/2024 09:17AM CT	enumeration	Completed reviewing HTTP services.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-headers.
10/09/2024 09:17AM CT	enumeration	Completed analyzing web services running on port 8080/tcp.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-robots.txt.
10/09/2024 09:17AM CT	enumeration	Completed reviewing HTTP services.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: smb-enum-shares.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-shellshock.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-title.
10/09/2024 09:17AM CT	enumeration	Analyzing web services running on port 80/tcp.
10/09/2024 09:17AM CT	enumeration	MITRE | ATT&CK Enumerating operating systems.
10/09/2024 09:17AM CT	enumeration	Completed analyzing web services running on port 443/tcp.
10/09/2024 09:17AM CT	enumeration	Completed checking OWA web apps for the ProxyShell vulnerability.
10/09/2024 09:17AM CT	enumeration	Completed reviewing HTTPS services.
10/09/2024 09:17AM CT	enumeration	Completed nmap script scan using script: http-methods.
10/09/2024 09:17AM CT	enumeration	Queuing up MSF module: auxiliary/scanner/smb/smb_ms17_010.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/ftp/ftp_version.

10/09/2024 09:17AM CT	enumeration	Completed reviewing FTP services.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/telnet/telnet_version.
10/09/2024 09:17AM CT	enumeration	Completed enumerating Telnet services.
10/09/2024 09:17AM CT	enumeration	Completed MSF module: auxiliary/scanner/smb/smb_ms17_010.
10/09/2024 09:17AM CT	enumeration	Checking if SMB servers allow SMB NULL authentication.
10/09/2024 09:17AM CT	enumeration	Attempting to enumerate SMB ports.
10/09/2024 09:17AM CT	enumeration	Completed enumerating SMB services.
10/09/2024 09:17AM CT	enumeration	Completed analyzing web services running on port 80/tcp.
10/09/2024 09:17AM CT	enumeration	Completed reviewing HTTP services.
10/09/2024 09:17AM CT	enumeration	Attempting to enumerate domain user accounts via username guessing.
10/09/2024 09:17AM CT	enumeration	Identified domain: [obfuscated-domain].local
10/09/2024 09:17AM CT	enumeration	Targeting domain "[obfuscated-domain].local" via 10.10.1.202 ([obfuscated-dns]).
10/09/2024 09:17AM CT	enumeration	Identified 59 valid domain user accounts.
10/09/2024 09:17AM CT	enumeration	Completed domain user enumeration module.
10/09/2024 09:17AM CT	enumeration	Started analyzing discovered web services to check for potentially interesting instances.
10/09/2024 09:17AM CT	enumeration	Completed analysis of web services.
10/09/2024 09:17AM CT	enumeration	Enumeration module completed.
10/09/2024 09:17AM CT	exploit	Launching exploit module.
10/09/2024 09:17AM CT	enumeration	Launching VNC login attack against five (5) VNC servers.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: auxiliary/scanner/vnc/vnc_login.
10/09/2024 09:17AM CT	exploit	Completed MSF module: auxiliary/scanner/vnc/vnc_login.
10/09/2024 09:17AM CT	enumeration	No VNC servers were found to accept default credentials.
10/09/2024 09:17AM CT	exploit	Starting the SMB login exploit module.
10/09/2024 09:17AM CT	exploit	MITRE | ATT&CK Targeting 59 of 59 user accounts for a single password attack to test for weak credentials.
10/09/2024 09:17AM CT	exploit	Queuing up CrackMapExec attack: cme_initial_smb_login_attack against 10.10.1.202 ([obfuscated-dns]).
10/09/2024 09:17AM CT	exploit	Completed CrackMapExec attack targeting smb.
10/09/2024 09:17AM CT	exploit	The password attack identified 0 successful login attempts and 59 failed login attempts.
10/09/2024 09:17AM CT	exploit	Completed the SMB login exploit module.
10/09/2024 09:17AM CT	exploit	Analyzing one (1) system that was vulnerable to the RCE exploit called Bluekeep (CVE-2019-0708).
10/09/2024 09:17AM CT	exploit	Exploitation of BlueKeep will not be attempted because the vulnerable system cannot be safely targeted.
10/09/2024 09:17AM CT	exploit	Launching the Metasploit module `opensmtpd_mail_from_rce` with the check option against five (5) default SMTP ports to check for the presence of OpenSMTPD servers that could be vulnerable to CVE-2020-7247.
10/09/2024 09:17AM CT	exploit	MITRE | ATT&CK Performing password attack against MSSQL services.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: auxiliary/scanner/mssql/mssql_login.
10/09/2024 09:17AM CT	exploit	Completed MSF module: auxiliary/scanner/mssql/mssql_login.
10/09/2024 09:17AM CT	exploit	Completed MSSQL password attacks.
10/09/2024 09:17AM CT	exploit	MITRE | ATT&CK Performing password attack against MSSQL services.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: auxiliary/scanner/mysql/mysql_login.

10/09/2024 09:17AM CT	exploit	Completed MSF module: auxiliary/scanner/mysql/mysql_login.
10/09/2024 09:17AM CT	exploit	Completed MySQL password attack.
10/09/2024 09:17AM CT	enumeration	Completed Firebird default credentials check.
10/09/2024 09:17AM CT	enumeration	Launching FTP login attack with random credentials against 1 FTP server not accpeting anonymous FTP authentication.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: auxiliary/scanner/ftp/ftp_login.
10/09/2024 09:17AM CT	exploit	Completed MSF module: auxiliary/scanner/ftp/ftp_login.
10/09/2024 09:17AM CT	enumeration	Completed exploit attempts against FTP services.
10/09/2024 09:17AM CT	enumeration	Identified potential Hikvision web instances. Scanning them for vulnerabilities.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: auxiliary/gather/hikvision_info_disclosure_cve_2017_7921.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: exploit/linux/http/hikvision_cve_2021_36260_blind.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: auxiliary/gather/hikvision_info_disclosure_cve_2017_7921.
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: exploit/linux/http/hikvision_cve_2021_36260_blind.
10/09/2024 09:17AM CT	exploit	Completed MSF module: exploit/linux/http/hikvision_cve_2021_36260_blind.
10/09/2024 09:17AM CT	exploit	Completed MSF module: auxiliary/gather/hikvision_info_disclosure_cve_2017_7921.
10/09/2024 09:17AM CT	exploit	Completed MSF module: auxiliary/gather/hikvision_info_disclosure_cve_2017_7921.
10/09/2024 09:17AM CT	exploit	Completed MSF module: exploit/linux/http/hikvision_cve_2021_36260_blind.
10/09/2024 09:17AM CT	exploit	MITRE ATT&CK Running DNS poisoner module.
10/09/2024 09:17AM CT	exploit	Deploying rogue DHCPv6 server.
10/09/2024 09:17AM CT	exploit	Logging activities from DNS poisoner.
10/09/2024 09:17AM CT	exploit	Logging activities from IPv6 attack.
10/09/2024 09:17AM CT	exploit	Skipping [obfuscated dns]$ username due to computer account detection.
10/09/2024 09:17AM CT	exploit	Obtained 1 new hashes due to DNS poisoning attacks.
10/09/2024 09:17AM CT	exploit	Identified SAM database files due to successful ntlmrelay attacks. Attempting to identify local administrator password reuse across one (1) system.
10/09/2024 09:17AM CT	exploit	Identifying if any local administrator credentials exist for 10.10.9.164 ([obfuscated-dns]).
10/09/2024 09:17AM CT	exploit	No local administrator password reuse identified.
10/09/2024 09:17AM CT	exploit	MITRE ATT&CK Launching password cracking instance.
10/09/2024 09:17AM CT	exploit	Successfully cracked one (1) password hash. Retrieving credentials.
10/09/2024 09:17AM CT	exploit	Completed hashcat password cracking session.
10/09/2024 09:17AM CT	exploit	Queueing user [obfuscated-domain].local\[obfuscated username] for credential validation against 10.10.0.140 ([obfuscated-dns]).
10/09/2024 09:17AM CT	exploit	Queuing up MSF module: auxiliary/scanner/smb/smb_login.
10/09/2024 09:17AM CT	exploit	Completed MSF module: auxiliary/scanner/smb/smb_login.
10/09/2024 09:17AM CT	exploit	Successfully identified valid credentials for [obfuscated-domain].local\[obfuscated username] against 10.10.0.140 ([obfuscated-dns]).
10/09/2024 09:17AM CT	exploit	Completed DNS poisoning attacks.
10/09/2024 09:17AM CT	exploit	Completed exploit module.
10/09/2024 09:17AM CT	complete	Assessment is complete and reports are available.